

Entorno personal de aprendizaje:

Curso de Ciberseguridad: Seguridad en medios digitales



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

 **GOBIERNO
NACIONAL**

*Paraguay
de la gente*

Unidad 5. Seguridad en Equipos

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Viceministerio de Tecnologías de la Información y Comunicación

Director General de Inclusión Digital y TIC en la Educación

Dirección General de Ciberseguridad y Protección a la Información

SEDE 1



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

Dirección: Complejo Santos E2 - Gral. Santos 1170 c/ Concordia

Teléfono: (+595 21) 217 9000

Correo electrónico: comunicacion@mitic.gov.py

Mesa de entrada: sgeneral@mitic.gov.py

Asunción – Paraguay

Entorno personal de aprendizaje (PLE):
Curso de Ciberseguridad: Seguridad en medios digitales

Todas las imágenes presentes en este material de apoyo educativo han sido reconocidas y, en todos los casos, son de uso libre. Todas las fuentes bibliográficas utilizadas en este material de apoyo educativo son citadas mediante el gestor de referencias bibliográficas Zotero, desarrollado por el Center for History and New Media de la Universidad George Mason, utilizando el estilo de la American Psychological Association Séptima Edición.

1. Riesgos en los Equipos

1.1. Vulnerabilidades en aplicaciones

Los equipos informáticos, tales como computadoras, dispositivos móviles, etc. constan de dos componentes fundamentales:

- Sistema operativo: Windows, Linux, OS X, Android, etc.
- Programas o aplicaciones: Office, Java, los navegadores, etc.

Tanto el sistema operativo como los programas tienen fallas de seguridad o vulnerabilidades, las cuales son descubiertas frecuentemente y que deben ser corregidas. Finalmente, cualquier programa es un conjunto de líneas de código de programación, programadas por humanos, que como tal, somos imperfectos y cometemos errores.



Muchas veces los ataques cibernéticos se centran en encontrar estas fallas de seguridad en nuestros equipos para explotarlas e ingresar así a nuestros sistemas y acceder a nuestra información. Para esto, normalmente los atacantes diseñan programas maliciosos, denominados de forma genérica malware (software malicioso).

2.El Malware y el Rasomware

2.1. Concepto

Malware o “software malicioso” es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas. Los malware se clasifican en virus, troyanos, spyware y muchos otros tipos, de acuerdo a sus características. Muchas veces llamamos erróneamente "virus" a todos ellos. En realidad, el virus es una categoría solamente; el término correcto es malware o software malicioso.

Si bien, no vamos a profundizar en las diferencias entre estas categorías ni en sus múltiples formas de clasificación técnicas, vamos a destacar que cada malware puede tener diferentes fines u objetivos, a veces incluso un único malware puede tener múltiples propósitos, entre los cuales podemos citar algunos:

- Robo de información personal, confidencial, financiera, etc.
- Realizar ataques de denegación de servicio a otros
- Utilizar el procesamiento de la máquina infectada para minar bitcoins u otros fines
- Ser el punto de entrada a una red a la cual la máquina tiene acceso
- Ser un punto de alojamiento/distribución de más software malicioso
- Cifrar nuestra información para obtener un pago a modo de rescate

Esto último corresponde a la clasificación de ransomware, un tipo de software malicioso que ha aumentado drásticamente en los últimos años, que “secuestra” nuestros archivos: los encripta y nos exige un pago para desencriptarlos.



Unidad 5.

Seguridad en Equipos

El malware, al igual que la gran mayoría de las amenazas que hemos visto hasta ahora, pueden afectar a cualquier tipo de equipo: PC, notebook, tablet, smartphones, etc. Igualmente, pueden afectar a cualquier sistema operativo: Windows, OS X (Mac), Linux, Android, etc. Si bien, existe un mito que los virus no afectan a Linux ni a Mac, esto no es del todo cierto: primeramente, hay que recordar que el virus es solo una categoría. Qué hay de los troyanos, spyware, ransomware? Si bien, los malware para Linux y Mac tienen características técnicas diferentes, sí que existen.

2.2. Ransomware

El ransomware es un tipo de malware, cuyo nombre viene de la palabra ransom en inglés, "rescate", justamente porque se trata de un secuestro virtual de la información de la víctima. El malware al ejecutarse cifra todos los archivos del equipo (y a veces incluso de otras máquinas de la red) con una clave que solamente conoce el atacante, quien nos exige dinero a cambio de proporcionarnos la clave y devolvernos el acceso a nuestros archivos.



Unidad 5.

Seguridad en Equipos

Existen miles de familias y variantes de ransomware: Cryptolocker, Teslacrypt, Wallet, WannaCry, Cerber, y muchos otros más. Si bien, es un programa malicioso que se ejecuta en un equipo, el daño real no es al equipo, sino a la información. Incluso, seríamos capaces de eliminar el malware (ya sea de forma manual, con un antivirus o incluso formateando el equipo), sin embargo, los archivos seguirían cifrados.

Como lo veremos en el Módulo de Protección de los Datos, la criptografía es una ciencia que nos permite, a través de algoritmos matemáticos, proteger la información, tal que nadie que no conozca la clave con la que se cifró la información, lo pueda leer. Los cibercriminales utilizan la criptografía, no para proteger la información, sino para impedirle el acceso a la información a las víctimas. Es por ello que, en alrededor del 90% de los casos, no hay una forma de recuperar la información cifrada sin la clave, que solo la conocen los atacantes.

Actualmente la tendencia entre los criminales y bandas que se dedican al ransomware es buscar atacar no solamente a usuarios individuales sino incluso a organizaciones enteras, desde PYMEs hasta grandes empresas, en donde el impacto por la pérdida de la información es mayor, y por ende, la víctima es más propensa a acceder al pago. Últimamente se ha observado también muchos casos de ransomware que amenazan a la víctima a publicar la información, buscando dañar su reputación.

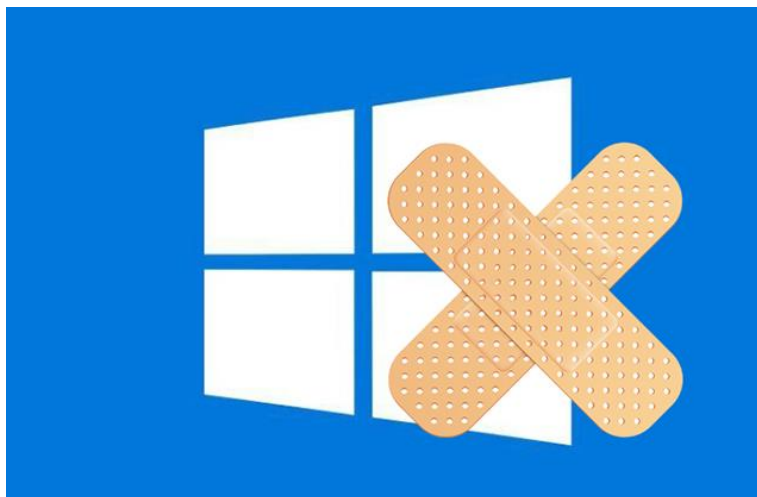
La mejor defensa ante ransomware es contar con una estrategia de resguardo y copias de seguridad de la información. Tenemos que tener en cuenta que no es suficiente con tener una copia de seguridad, sino tenerla en un equipo o sistema separado del sistema original (preferentemente, al menos una copia, offline). En el Módulo de Protección de los Datos mostraremos algunas posibles estrategias y herramientas.

En algunos casos, se descubre una manera de recuperar los archivos, ya sea porque se dieron a conocer las claves (los cibercriminales las publican, las fuerzas de aplicación de ley atrapan a las bandas criminales, u otros escenarios posibles, pero poco frecuentes), o porque se descubrió una falla en el ransomware, que permitió recuperar las claves o los archivos. Recordemos que el malware no es otra cosa que un programa, malicioso, escrito por humanos por lo que, como todo programa, también tienen fallas.

3. Vulnerabilidades

3.1. Mecanismos de protección

Existen múltiples formas de quedar infectado con un malware o, en general, ser víctima de una intrusión u otro tipo de ataques: mediante un adjunto malicioso que nos llega por correo, navegando a través de una página web que contiene código malicioso, a través de un pen drive, etc.



Las vulnerabilidades son fallos en un programa, son errores en el código o en la configuración de estos. Todos los días se descubren vulnerabilidades que afectan a todo tipo de programas: desde el sistema operativo, ya sea Windows, Linux, OS X, Android, etc., hasta a los programas y aplicaciones como Office, Adobe Reader, los navegadores y sus plugins, Java, y absolutamente cualquier otro programa que utilicemos. Algunas de estas vulnerabilidades son críticas, otras son errores menores, que, dependiendo del contexto, pueden o no ser aprovechadas por un atacante.

Las vulnerabilidades se corrigen mediante las actualizaciones o "parches". Estas actualizaciones son las correcciones a los errores que se descubren. Si no actualizamos absolutamente TODO nuestro software, esos errores quedarán sin corregir y, eventualmente, algún atacante las aprovechará. Por ello, la actualización permanente es fundamental. Casi todos de los sistemas operativos y programas permiten la actualización automática, la cual en la mayoría de los casos puede ser una gran ayuda, de modo a que no tengamos que

Unidad 5. Seguridad en Equipos

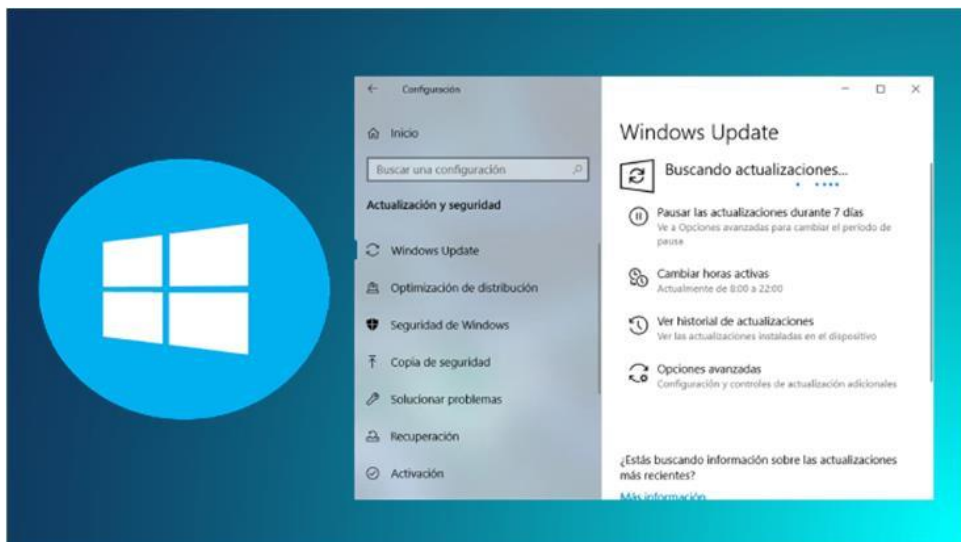
acordarnos todos los días de revisar la versión ni descargar parches de forma manual: el proceso es automático y transparente para el usuario.

4. Actualizaciones

4.1. Concepto

Cuando una vulnerabilidad es descubierta, el fabricante del producto afectado normalmente la corrige a través de lo que llamamos un parche o actualización. Es fundamental aplicar estas actualizaciones de modo a proteger nuestros sistemas y nuestra información.

Hoy en día, la mayoría de los sistemas operativos y programas ofrecen la posibilidad de chequear e instalar las actualizaciones de forma automática. Esto nos facilita enormemente el proceso de buscar las actualizaciones, descargarlas e instalarlas manualmente. Además, evita que descarguemos actualizaciones no oficiales que muchas veces son programas maliciosos.



Es importante resaltar que, en algunas organizaciones, no se permite la actualización automática debido a que existen aplicaciones o sistemas específicos no soportados oficialmente por el proveedor de la actualización, por lo que podría haber problemas de compatibilidad. Además, por una racionalización del ancho de banda y gestión de la red, a veces se aplican políticas de restricción de horario de descarga. Sin embargo, en la gran mayoría de los casos,

Unidad 5.

Seguridad en Equipos

especialmente en equipos de usuarios finales, la actualización automática no creará mayores problemas, por lo que, en caso de ser posible, se debería optar por esta opción.

Tenemos que tener en cuenta que, si no tenemos una licencia legal y activa de un software, no tendremos acceso a las actualizaciones. Si alguna vez has utilizado por ejemplo un Windows "pirata" o "crackeado", habrás notado que el Windows Update está desactivado, o que falla cada vez que se intenta actualizar. Por ello, las fallas de seguridad que se descubran, quedarán expuestas y aumenta la probabilidad de quedar infectado con malware.

5. Software de Seguridad

5.1. Concepto

Actualmente, la mayoría de los antivirus se convirtieron en suites de seguridad, que integran varias funciones, además de la detección de virus: firewall, anti-malware, sistema de detección de incidente basado en host, backup, antirrobo, entre muchas otras. Aun así, frecuentemente se le sigue denominando “antivirus” simplemente.



Los **firewalls** o cortafuegos, programas **antivirus** y programas **antimalware** trabajan en conjunto y deben utilizarse para proveer el máximo nivel de seguridad para proteger la computadora. Anteriormente la mayoría de las soluciones antivirus se limitaban a analizar los archivos de nuestro disco. Sin embargo, hoy en día, la industria de seguridad evolucionó

Unidad 5.

Seguridad en Equipos

enormemente, y no se limita a esto, sino que busca protegernos de forma proactiva de manera a prevenir los diversos tipos de ataques.

Firewall: Un firewall ayuda a prevenir que la información entre o salga de nuestra computadora sin nuestra autorización, controlando lo que es visible desde Internet y bloqueando las comunicaciones de fuentes no autorizadas. Cada computadora que está conectada a Internet debe tener un firewall activado en todo momento. Muchos sistemas operativos ya vienen con firewalls integrados, como en el caso de Windows. Sin embargo, existen soluciones más avanzadas, ya sea integradas a soluciones antivirus o soluciones independientes. En caso de que optemos por estas soluciones, se debe desactivar el firewall del sistema operativo, delegando esta función a la solución que elegimos.

Antivirus: Los programas antivirus de software ayudan a proteger nuestros equipos de malware que pueden destruir datos, robar información y datos personales y/o hacer que el equipo no funcione correctamente y sea más lento. El software antivirus escanea su computadora para detectar patrones que pueden indicar que el aparato ha sido infectado. Estos patrones se basan en firmas, definiciones o virus que ya son conocidos. Todos los días se descubren alrededor de 400.000 nuevas variantes de malware. Por lo tanto, es importante contar siempre con el antivirus actualizado, de modo a contar con las últimas definiciones o firmas. Esto muchas veces sólo está disponible en las versiones de pago.

Existen muchas compañías que producen software antivirus. Algunos de los más conocidos son:

- **ESET Smart Security** - <http://www.eset-la.com/hogar>
- **Kaspersky Antivirus** - <http://latam.kaspersky.com/productos/productos-para-el-hogar/anti-virus>
- **Norton Security** - <http://es.norton.com/norton-security-antivirus>
- **Avast** - <https://www.avast.com/es-ww/index#compare-home>
- **Microsoft Security Essentials** - <http://windows.microsoft.com/en-us/windows/security-essentials-download>

Unidad 5.

Seguridad en Equipos

Si bien, la mayoría de los antivirus están disponibles para sistemas operativos Windows, cada día existen más antivirus para otros sistemas operativos como Mac OS X y Android. Se debe tener en cuenta que las amenazas de seguridad existen, en mayor o menor medida, en todos los sistemas operativos, por lo que es recomendable contar con soluciones antivirus en todos los sistemas operativos.

Anti malware: La palabra malware abarca una amplia categoría de amenazas incluyendo spyware (software espía), adware (software publicitario), caballos de Troya y otros programas no deseados que podrían ser instalados en nuestra computadora sin nuestro conocimiento o consentimiento. Estos programas maliciosos no se definen como “virus”, pero pueden ser igual o más dañinos. El spyware, por ejemplo, puede recopilar nuestra información a través de Internet sin que lo notemos, interceptando prácticamente cualquier dato: actividad en Internet, correos electrónicos, contactos y lo que escribimos.

Los programas anti malware y anti spyware ayudan a eliminar muchas de estas amenazas. Los siguientes son ejemplos de sitios que ofrecen programas gratuitos de anti malware:

- **Malwarebytes** - <http://es.malwarebytes.org>
- **Super Anti-Spyware** - www.superantispyware.com
- **Spybot Search and Destroy** - www.safer-networking.org/en/index.html

Obs.: Al igual que los antivirus y las suites de seguridad, estos programas cuentan con funcionalidades básicas en sus versiones gratuitas o de prueba. Para acceder a una protección más completa y proactiva, se recomienda utilizar las versiones de pago.

Unidad 5.

Seguridad en Equipos



La mayoría del software de seguridad pre-instalado en computadora solamente funciona por un pequeño período de tiempo de prueba; para acceder a todas las funcionalidades de un antivirus normalmente se debe pagar una suscripción. El software de seguridad solamente nos protege contra amenazas nuevas si está actualizado, lo cual suele ser una característica reservada a las versiones de pago, por lo cual siempre se recomienda invertir en este tipo de soluciones.

Aunque la mayoría de los programas antivirus también tienen la capacidad de combatir malware, debido a la creciente sofisticación de los programas de malware, lo mejor es utilizar un programas anti malware además de un programa antivirus. Cada uno se especializa en detectar amenazas ligeramente distintas, por lo tanto, siempre es recomendable utilizarlos de forma conjunta para una mayor seguridad.

6. Buenas Prácticas

Resumimos algunas buenas prácticas para mantener nuestros equipos seguros:

1. No descargar programas de dudosa reputación. Softonic, Taringa, y otros programas de descarga no son sitios confiables ni ofrecen garantías de que el software descargado sea legítimo. En el caso de teléfonos móviles, asegúrate de instalar solamente aplicaciones desde la tienda de aplicaciones oficiales (Google Play o App Store de Apple).
2. Utilice siempre sistemas operativos y software original. Las versiones no originales (“piratas”) o modificadas (“crackeadas”) la mayoría de las veces no pueden acceder a las actualizaciones de seguridad, por lo que las fallas de seguridad descubiertas quedan expuestas y aumenta la probabilidad de quedar infectado con malware. Además, muchas veces el software ilegal contiene software malicioso que se instala sin que el usuario lo sepa.
3. El correo de spam y phishing suele estar relacionado con la distribución de malware, por lo que es importante tomar las precauciones al entrar a los enlaces y/o abrir los adjuntos presentes en este tipo de mensajes.
4. Mantener el sistema operativo y todos los programas actualizados.
5. Deshabilitar las carpetas compartidas siempre que sea posible. Esto evita la propagación de gusanos que aprovechen ese vector como método de infección.
6. Deshabilitar la ejecución automática de dispositivos USB. Los dispositivos de almacenamiento removibles que se conectan al puerto USB constituyen un vector de ataque muy empleado por el malware para la propagación, sobre todo, de gusanos.
7. Contar con soluciones de antivirus, antimalware y/o firewall.